UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

Todd Joseph Elliot, individually, and on behalf of all others similarly situated,	*	Civil Action No. __
	*	CLASS ACTION COMPLAINT
Plaintiff,	*	
vs.	*	
Marriott International, Inc.,	*	JURY TRIAL DEMANDED
Defendant.	*	

COMPLAINT

For his complaint against the defendant Marriott International, Inc. ("Marriott"), Plaintiff Todd Joseph Elliot (hereinafter "Plaintiff") alleges, in his own right and on behalf of all others similarly situated, as follows:

NATURE OF THE ACTION

1. This is a class action on behalf of consumers injured as a result of a massive security breach of Marriott's Starwood guest reservation database that began in or around 2014 (hereinafter, the "Marriott Data Breach"). As a result of the Marriott Data Breach, personal and financial information belonging to up to 500 million customers was compromised.

2. At the time of the Marriott Data Breach, Marriott failed to maintain reasonable security measures to protect its guests' personal and financial information, including payment card numbers and expiration dates, mailing addresses, phone numbers, email addresses, passport numbers, dates of birth, and gender. The Marriott Data Breach was a direct, foreseeable result of Marriott's security failures.

3. Marriott's failure to adequately protect its guests' personal information is particularly unreasonable in light of the many other well-publicized data breaches in recent years, including Target, Home Depot, Yahoo, and Equifax.

4. This action is brought on behalf of all persons in the United States whose personal and financial information was compromised as a result of the Marriott Data Breach.

FACTUAL BACKGROUND

5. Marriott was founded in 1927, and it became the largest hotel operator in the world when it purchased Starwood Hotels & Resorts Worldwide for $13 billion in 2016.[1] In its 2017 Annual Report, Marriott claimed operating revenue totaling $22.894 billion and operating income of $2.359 billion.[2]

6. On November 30, 2018, Marriott first disclosed that its "Starwood guest reservation database" had been hacked.[3] The company stated it received an alert from an internal security tool on September 8, 2018 about an "attempt to access" the Starwood guest reservation database in the United States.[4] Marriott commenced an investigation and determined on November 19, 2018 that unauthorized access to the database had occurred.[5]

7. Shockingly, the investigation revealed that there had been unauthorized access to the Starwood network as far back as 2014.[6]

8. Marriott admits that its database contains information belonging to up to 500 million guests

[1] *See* https://www.forbes.com/sites/halahtouryalai/2018/06/06/worlds-biggest-hotels-2018/#5df6e54e47c7)(last accessed Nov. 30, 2018).
[2] *See* https://marriott.gcs-web.com/static-files/b82978a6-9d28-4e38-9855-fc4ae2cebe11 (last accessed Nov. 30, 2018).
[3] *See* http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (last accessed Nov. 30, 2018).
[4] *Id.*
[5] *Id.*
[6] *Id.*

who made reservations at a Starwood property, and that for approximately 327 million of those guests, "the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences."[7]

9. Additionally, for an unknown number of guests, the hacked information also includes payment card numbers and payment card expiration dates. Marriott has "not been able to rule out the possibility" that both pieces of payment card information were taken by the hackers.[8]

10. As NBC News reports: "The breach could potentially be one of the largest in history, behind the hacking of about 3 billion Yahoo accounts."[9]

11. The massive data breach could have been prevented and should have been detected and disclosed by Marriott earlier. In November 2015, just days after being acquired by Marriott, Starwood disclosed its own breach involving more than 50 properties.[10] At that time, Starwood stated that the breach stretched back at least one year—to November 2014.[11]

12. Yet despite Starwood's public disclosure of that breach,Marriott neglected to take the steps necessary to remedy Starwood's vulnerable database system—or to do so in a timely fashion. The result is the massive data breach that is the subject of this complaint, with serious consequences likely to follow—perhaps for decades—for some 500 million customers.

13. In an extreme example of the idiom "too little too late," given Marriott's knowledge of the

[7] *Id.*
[8] *Id.*
[9] *See* *https://www.nbcnews.com/tech/security/marriott-says-data-breach-compromised-info-500-million-guests-n942041* (last accessed Nov. 30, 2018).
[10] *See* https://krebsonsecurity.com/2015/11/starwood-hotels-warns-of-credit-card-breach/ (last accessed Nov. 30, 2018).
[11] *Id.*

Starwood system's vulnerabilities at the time of its acquisition in 2015, Marriott President and Chief Executive Officer Arne Sorenson stated on November 30, 2018:[12]

> Finally, we are **devoting the resources necessary to phase out Starwood systems** and accelerate the ongoing security enhancements to our network. . . . .[13]

14. Marriott did not do nearly enough to protect its guests' data, particularly given its extraordinary financial resources.

15. As a result of Marriott's inadequate and unreasonable data security, cyber-criminals now possess the personal and financial information of Plaintiff and the Proposed Class. Unlike credit card data breaches, like those recently at Target Corp. and Home Depot, the harm here cannot be attenuated by cancelling and reissuing credit cards. With names, addresses, birthdates, credit information, and possibly social security numbers ("SSN"), criminals can open entirely new credit accounts and bank accounts, and garner millions of dollars through fraud that victims will not be able to detect until it is too late. Victims' credit profiles can be destroyed and they will lose the ability to legitimately borrow money, obtain credit, or even open bank accounts.

16. Further, criminals can file false federal and state tax returns in victim's names, preventing or at least delaying victims' receipt of their legitimate tax refunds and potentially making victims targets of IRS and state tax investigations. At the very least, victims must add themselves to credit fraud watch lists, which substantially impair victims' ability to obtain additional credit. Many experts advise a flat out freeze on all credit accounts, making it impossible to rent a car, get student loans, or buy or rent furniture or a new TV, let alone complete a major purchase such as a new car or home, without taking the time to request that the freeze be suspended, waiting the days it can

[12] *Id.* (emphasis added).
[13] *See* http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (last accessed Nov. 30, 2018).

take for that to occur, and then reinstating the freeze.

17. Additionally, there are four major reporting agencies, so consumers may need to take these steps with all of them because they will not know which bureau a creditor may consult.

18. Immediate notice of a data breach is essential to obtain the best protection afforded by identity theft protection services. Marriott failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the Proposed Class resulting from the breach. The breach began more than four years ago, sometime in 2014. Marriott learned of the breach on September 8, 2018. Yet, Marriott did not disclose the breach to its customers until November 30, 2018. Such delay was unwarranted and directly increases the likelihood that thieves have already stolen or will be able to steal victims' identities before victims even know that they are at risk.

19. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites. A credit card number trades for under $10 on the black market. Magnetic track data increases the price, and a card with full personal information such as an address, phone number, and email address ("fullz") are traded at around $25 per record.[14]

20. But this breach is far more valuable. The data breach consists of over 500 million records that include names, mailing addresses, phone numbers, email addresses, passport numbers, dates of birth, and genders. Complete identity records can sell for up to $250 to $400 on the black market, making this a breach possibly worth billions of dollars to cybercriminals. It is not yet clear if customer social security numbers ("SSN") were compromised in the breach.

[14] Max Cherney, *It's Surprisingly Cheap to Buy Stolen Bank Details*, MOTHERBOARD (Dec. 23, 2013), available at https://motherboard.vice.com/en_us/article/nzewpx/its-surprisingly-cheap-to-buy-stolen-bank-details (last accessed Nov. 30, 2018).

21. The personal and financial information that Marriott failed to adequately protect are "as good as gold" to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, and file false federal and state tax returns.

22. Further, there is little Marriott can do to protect victims once the information is out. Credit monitoring services have limited ability to prevent wholesale identity theft. Moreover, experts warn that batches of stolen information will not be immediately dumped on the black market.

23. This is especially true if hackers accessed SSN, which unlike credit cards, are not reissued. A cybercriminal, especially one with millions of SSN records, can hold on to stolen information for years until the news of the theft has subsided, then steal a victim's identity, credit, and bank accounts, resulting in thousands of dollars in losses and lost time and productivity. Thus, Plaintiff and the Proposed Class must take additional steps to protect their identities. And Plaintiff and the Proposed Class must bear the burden and expense of identity and credit monitoring, and heightened vigilance for years to come.

PARTIES

24. Defendant Marriott International, Inc. is a corporation with its principal place of business in Bethesda, Montgomery County, Maryland.

25. Plaintiff Todd Joseph Elliot is a Louisiana resident. Plaintiff is a Marriott customer who has used the Starwood reservation system. Because Marriot has reported that some 500 million customer accounts were compromised, it is virtually certain that plaintiff Elliot's data was impacted.

JURISDICTION AND VENUE

26. This Court has diversity jurisdiction over this action under the Class Action Fairness Act,

28 U.S.C. § 1332(d)(2). Plaintiff and Defendant are citizens of different states. The amount in controversy exceeds $5 million, exclusive of interest and costs, and there are more than 100 putative class members.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Marriott regularly conducts business and resides in this district; a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims were committed in this district; and property that is the subject of the Plaintiff's claims are in this district.

CLASS ALLEGATIONS

28. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action as a class action for himself and all members of the following Proposed Class of similarly situated individuals and entities:

> All persons in the United States whose personal and financial information was accessed, compromised, or stolen as a result of the data breach first disclosed by Marriott on or about November 30, 2018.

29. Excluded from the Proposed Class are the Defendant, including any entity in which Defendant has a controlling interest, which is a parent or subsidiary, or which is controlled by the Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

30. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

31. All members of the Proposed Class are readily ascertainable. Marriott has access to addresses and other contact information for all members of the Proposed Class, which can be used for providing notice to Proposed Class members.

32. ***Numerosity***. The Proposed Class is so numerous that joinder of all members is unfeasible and not practical. While the precise number of Proposed Class members has not been determined at this time, Marriott has admitted that some 500 million records were breached. Therefore, the individuals impacted will be sufficiently numerous to merit class certification.

33. ***Commonality***. Questions of law and fact common to all Proposed Class members exist and predominate over any questions affecting only individual Proposed Class members, including, *inter alia*, whether Marriott:

a. Engaged in the wrongful conduct alleged herein;

b. Acted in a manner that was deceptive, unfair, and/or unlawful;

c. Owed a duty to Plaintiff and members of the Proposed Class to adequately protect their personal and financial information;

d. Owed a duty to provide timely and accurate notice of the data breach to Plaintiff and members of the Proposed Class;

e. Used reasonable and industry-standard measures to protect Proposed Class members' personal and financial information;

f. Knew or should have known that its data system was vulnerable to attack;

g. Acted (or failed to act) in a manner that resulted in (or was the proximate cause of) the breach of its systems, which resulted in the loss of hundreds of millions of Proposed Class members' personal and financial data;

h. Should have notified the public immediately after it learned of a possible data breach;

i. Violated state statutory consumer protection, consumer fraud, data-breach-notification, and other applicable laws;

j. Marriott violated state common law as to negligence and otherwise violated Maryland common law; and

k. Is liable unto Plaintiff and the Proposed Class members for actual damages, statutory damages, and/or punitive damages, restitution, disgorgement, and/or other equitable relief.

34. ***Typicality***. Plaintiff's claims are typical of the claims of the Proposed Class. Plaintiff and all Proposed Class members were injured through the uniform misconduct described above and assert the same claims for relief.

35. ***Adequacy***. Plaintiff and his counsel will fairly and adequately represent the interests of the Proposed Class members. Plaintiff has no interest antagonistic to, or in conflict with, the interests of the Proposed Class members. Plaintiff's lawyers are highly experienced in the prosecution of consumer class actions and complex commercial litigation.

36. ***Superiority***. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiff and the Proposed Class members. Plaintiff and the proposed Class members have been harmed by Marriott's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Marriott's wrongful actions and/or inaction.

37. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual members of the Proposed Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

38. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2) because Marriott has acted or refused to act on grounds generally applicable to the Proposed Class, so that final

injunctive relief or corresponding declaratory relief is appropriate as to the Proposed Class as a whole.

39. The expense and burden of litigation would substantially impair the ability of Plaintiff and Proposed Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Marriott will retain the benefits of its wrongdoing despite its serious violations of the law.

SUBSTANTIVE GROUNDS FOR RELIEF

COUNT 1 – NEGLIGENCE

40. By accepting and storing Plaintiff's and the Proposed Class members' non-public personal and financial information, including highly sensitive information such as names, mailing addresses, phone numbers, email addresses, passport numbers, account information, dates of birth, and gender, Marriott assumed a duty, including a special or fiduciary duty, to Plaintiff and the Proposed Class and members requiring it to use reasonable and, at the very least, industry-standard care to secure such information against theft and misuse.

41. Marriott breached its duty of care by failing to adequately secure and protect Plaintiff's and the Proposed Class members' personal and financial information from theft, access, collection, and misuse by third parties.

42. Further, Marriott breached its duty of care by failing to act to protect Plaintiff's and the Class members' personal and financial information, including, upon information and belief, by neglecting to promptly, completely, and effectively patch and repair the Starwood system when initially advised of a breach in November 2015.

43. Marriott further breached its duty of care by failing to promptly, timely, clearly, accurately, and completely inform Plaintiff's and the Proposed Class that their personal and financial information had been stolen.

44. Plaintiff and members of the Proposed Class have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Marriott's negligence and misconduct.

45. As a direct and proximate result of Marriott's failure to take reasonable care and use, at a minimum, industry-standard measures to protect the personal information placed in its care, Plaintiff and members of the Proposed Class had their personal and financial information stolen, causing direct and measurable monetary losses, threat of future losses, identity theft, and threat of identity theft.

46. As a direct and proximate result of Marriott's negligence and misconduct, Plaintiff and members of the Proposed Class were injured in fact by: identity theft; the loss of the monetary value, including the market value, of their personal and financial information, due to the Marriott Data Breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT 2 – NEGLIGENCE PER SE

47. Plaintiff brings this count on his own behalf and on behalf of the Proposed Class under the laws of the state of Maryland.

48. Pursuant to Section 5 of the Federal Trade Commission Act ("FTC Act"), Marriott had a

duty to keep and protect the personal information of Plaintiff and Proposed Class members.

49. Marriott violated the FTC Act by failing to keep and protect Plaintiff and Proposed Class members' extremely sensitive and valuable personal and financial information, failing to monitor, and/or failing to ensure that it complied with data security standards, industry standards, statutes, and/or other regulations to protect such personal and financial information. All such omissions were patently unreasonable given the high stakes if malicious actors were to access such information, which they now have done.

50. Marriott violated the FTC Act by failing to safe-keep and protect Plaintiff's and Proposed Class members' personal and financial information, failing to monitor, and/or failing to ensure that Defendant complied with applicable and current data security standards, statutes, and/or other regulations to protect such personal and financial information.

51. Further, Marriott violated the FTC Act by failing to act to protect Proposed Class members' personal and financial information, including, upon information and belief, by neglecting to promptly patch and repair the Starwood system even after being aware that the system had been breached in November of 2014.

52. Marriott's failure to comply with the FTC Act constitutes negligence *per se*.

53. Plaintiff and members of the Proposed Class have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Marriott's negligence *per se*.

54. As a direct and proximate result of Marriott's negligence *per se*, Plaintiff and members of the Proposed Class had their personal and financial information stolen, causing direct and measurable monetary losses, threat of future losses, identity theft, and threat of identity theft.

55. As a direct and proximate result of Marriott's negligence *per se*, Plaintiff and members of

the Proposed Class were injured in fact by: identity theft; the loss of the monetary value, including the market value, of their personal and financial information, due to the Marriott Data Breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT 3 – VIOLATION OF THE MARYLAND CONSUMER PROTECTION ACT

56. Plaintiff and the Proposed Class members are "consumers" within the meaning of the Maryland Consumer Protection Act ("Maryland CPA"), Md. Code Comm. Law § 13-101, et seq.

57. Marriott is a merchant for purposes of Maryland's Consumer Protection Act. Marriott was, at all times relevant herein, engaged in soliciting "consumer services" as that term is defined in Md. Code Comm. Law § 13-101(d) by soliciting an ongoing service, credit reporting and data aggregation of Plaintiff's personal information, to consumers in Maryland for primarily personal use within the meanings specified in the Act.

58. Marriot is a "person" as that term is defined by Md. Code Comm. Law § 13-101(h), as Marriott was, at all times relevant herein, a legal or commercial entity.

59. Marriott, by failing to inform consumers, including Plaintiff and the Class Members, of Marriott's unsecure, uncompliant, and otherwise insufficient data and information security

practices, advertised, sold, serviced, and otherwise induced those consumers, including Plaintiff and Class Members, to purchase goods and services from Marriott.

60. By failing to inform consumers, including Plaintiff and the Class Members, that its data and information security practices were unsecure, uncompliant, and otherwise insufficient, Marriott falsely represented that its data and information security practices were sufficient to safeguard the personal and financial information of consumers, including Plaintiff and the Class Members.

61. Maryland law also requires timely notification of data breaches upon identification. Marriott identified the Data Breach on September 8, 2018, but did not notify consumers, including Plaintiff and the Class Members, until November 30, 2018.

62. Marriott's failures constitute false, misleading, and misrepresentations, which have the capacity, tendency, and effect of deceiving or misleading consumers, including Plaintiff and Class Members, concerning the security of their networks and aggregation of personal and financial information.

63. In addition, the facts upon which consumers, including Plaintiff and Class Members, relied were material facts, the veracity of which was not true (e.g., that their financial and personal data was adequately protected), and consumers, including Plaintiff and Class Members, relied on those false facts to their detriment.

64. Marriott employed these false representations to promote the sale of a consumer good or service, which Plaintiff and the Class Members purchased.

65. As a direct and proximate result of Marriott's violations of the Maryland Consumer Protection Statute, Plaintiff and members of the Proposed Class were injured in fact by: identity theft; the loss of the monetary value, including the market value, of their personal and financial

information, due to the Marriott Data Breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT 4 – VIOLATION OF THE MARYLAND PERSONAL INFORMATION PRIVACY ACT

66. This Count is brought pursuant to the Maryland Personal Information Privacy Act, Md. Code Comm. Law § 14-3504, et seq.

67. The Maryland Personal Information Privacy Act requires businesses that own or license personal information of an individual residing in the State to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.

68. Marriott failed to implement and maintain reasonable security procedures and practices appropriate to the nature of its customers' personal and financial information and the nature and size of Marriott and its operations.

69. Marriott's security failures constitute a violation of the Maryland Personal Information Privacy Act. A violation of that statute constitutes an unfair or deceptive trade practice within the meaning of the Maryland Consumer Protection Statute, and is subject to the enforcement and

penalty provisions of the Maryland Consumer Protection Statute. *See* Md. Code Comm. Law § 14-3508.

70. As a direct and proximate result of Marriott's violations of the Maryland Personal Information Privacy Act, Plaintiff and members of the Proposed Class were injured in fact by: identity theft; the loss of the monetary value, including the market value, of their personal and financial information, due to the Marriott Data Breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT 5 – VIOLATION OF THE MARYLAND SOCIAL SECURITY NUMBER PRIVACY ACT

71. This Count is brought pursuant to the Maryland Social Security Number Privacy Act, Md. Code Comm. Law § 14-3402.

72. The Maryland Social Security Number Privacy Act prohibits a person from publicly positing or displaying an individual's SSN or transmitting an individual's SSN over the Internet unless the connection is secure or the SSN number is encrypted. Md. Code Comm. Law § 14-3402(a).

73. As discussed above, Marriott failed to implement and maintain appropriate security procedures to protect its customers' personal and financial information.

74. As a result of Marriott's failure to implement and maintain appropriate security procedures, the Marriott Data Breach may have exposed customers', including Plaintiff's and Class Members', social security numbers "SSN" to unauthorized third parties in violation of the Maryland Social Security Number Privacy Act.

75. As a direct and proximate result of Marriott's violations of the Maryland Social Security Number Privacy Act, Plaintiff and members of the Proposed Class were injured in fact by: identity theft; the loss of the monetary value, including the market value, of their personal and financial information, due to the Marriott Data Breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT 6 – CONSTRUCTIVE FRAUD

76. At all times during Plaintiff's and Class Members' interactions with Marriott, Marriott was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' personal and financial information provided to Marriott.

77. As alleged herein and above, Marriott's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' personal and financial information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

78. Plaintiff and Class Members provided their respective personal and financial information to Marriott with the explicit and implicit understandings that Marriott would protect and not permit the information to be disseminated to any unauthorized parties.

79. Plaintiff and Class Members also provided their respective personal and financial information to Marriott with the explicit and implicit understanding that Marriott would take precautions to protect that information from unauthorized disclosure, such as following basic principles of information security practices.

80. Marriott voluntarily received in confidence Plaintiff's and Class Members' personal and financial information with the understanding that the information would not be disclosed or disseminated to the public or any unauthorized third parties.

81. Due to Marriott's failure to prevent, detect, and/or avoid the Data Breach from occurring by, failing to follow best information security practices to secure Plaintiff's and Class Members' personal and financial information, Plaintiff's and Class Members' Customer information was disclosed and misappropriated to unauthorized third parties.

82. But for Marriott's disclosure of Plaintiff's and Class Members' personal and financial information in violation of the parties' understanding of confidence, their information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Marriott's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' personal and financial information, as well as the resulting damages.

83. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Marriott's unauthorized disclosure of Plaintiff's and Class Members' personal and financial information.

84. As a direct and proximate result of Marriott's constructive fraud, Plaintiff and members of the Proposed Class were injured in fact by: identity theft; the loss of the monetary value, including

the market value, of their personal and financial information, due to the Marriott Data Breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

a. The proposed Class be certified, and that the named Plaintiff be named as Class Representative, and his counsel be appointed as Class Counsel;

b. Plaintiff and the Proposed Class be awarded appropriate relief, including actual and statutory damages, disgorgement, and restitution, punitive, exemplary, or multiple damages where available;

c. Plaintiff and the Proposed Class be awarded preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law;

d. Such additional orders or judgments as may be necessary to prevent these practices and to restore to any person in interest any money or property which may have been acquired by means of the violations; and

e. Plaintiff and the Proposed Class be awarded prejudgment and postjudgment interest;

f. Plaintiff and the Proposed Class be awarded reasonably attorneys' fees, costs, and

expenses;

g. Requiring Defendant to provide appropriate credit monitoring services to Plaintiff and the Proposed Class;

h. Plaintiff and the Proposed Class be awarded such other, favorable relief as may be available and appropriate under law or at equity.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all issues so triable.

DATED: November 30, 2018

Respectfully submitted,

/s/ *Joseph Musso*
Joseph Musso, Esq. (#07184)
Drew LaFramboise, Esq. (#20288)
Michelle Parfitt, Esq. (*pro hac vice* anticipated)
ASHCRAFT & GEREL LLP
4900 Seminary Road, Suite 650
Alexandria, VA 22311
Telephone: (703) 931-5501
Facsimile: (703) 824-4758
jmusso@ashcraftlaw.com
dlaframboise@ashcraftlaw.com
mparfitt@ashcraftlaw.com

Korey A. Nelson, Esq. (*pro hac vice* anticipated)
Amanda K. Klevorn, Esq. (*pro hac vice* anticipated)
C. Jacob Gower, Esq. (*pro hac vice* anticipated)
BURNS CHAREST LLP
365 Canal Street, Suite 1170
New Orleans, LA 70130
Telephone: (504) 799-2845
Facsimile: (504) 881-1765
knelson@burnscharest.com
aklevorn@burnscharest.com
jgower@burnscharest.com

Warren T. Burns, Esq. (*pro hac vice* anticipated)

Daniel H. Charest, Esq. (*pro hac vice* anticipated)
BURNS CHAREST LLP
900 Jackson Street, Suite 500
Dallas, Texas 75202
Telephone: (469) 904-4550
Facsimile: (469) 444-5002
wburns@burnscharest.com
dcharest@burnscharest.com